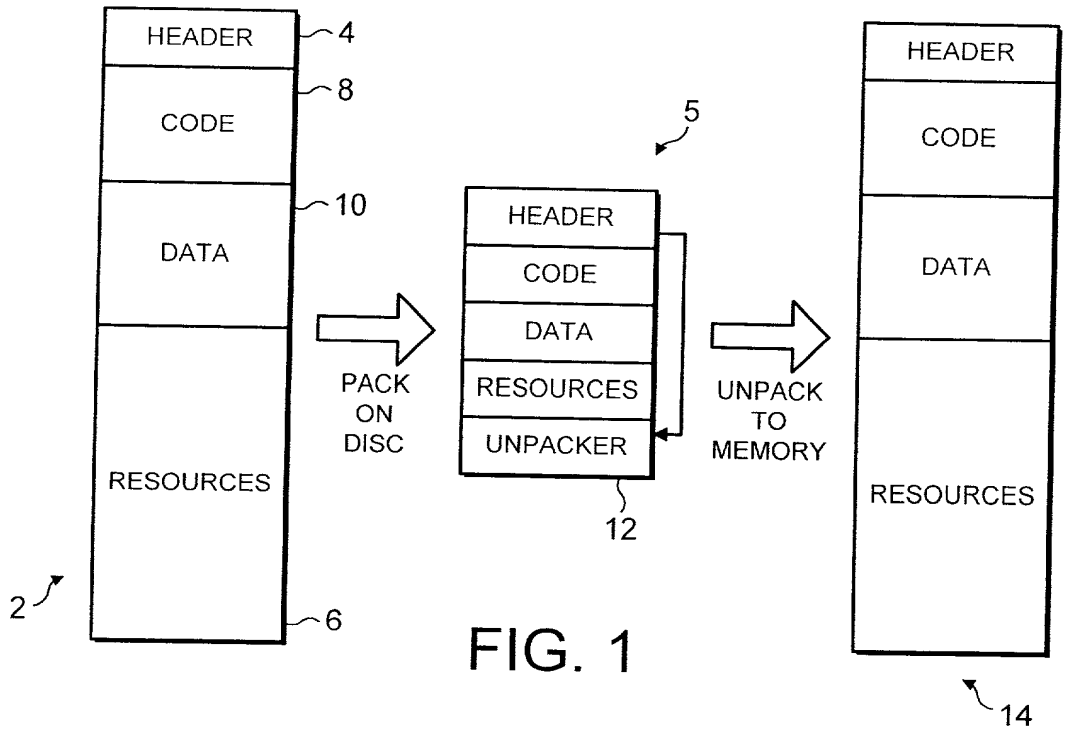

HEADER
4
CODE
8
DATA
10
RESOURCES
6
2
PACK
ON
DISC
5
HEADER
CODE
DATA
RESOURCES
UNPACKER
12
UNPACK
TO
MEMORY
HEADER
CODE
DATA
RESOURCES
14

FIG. 1

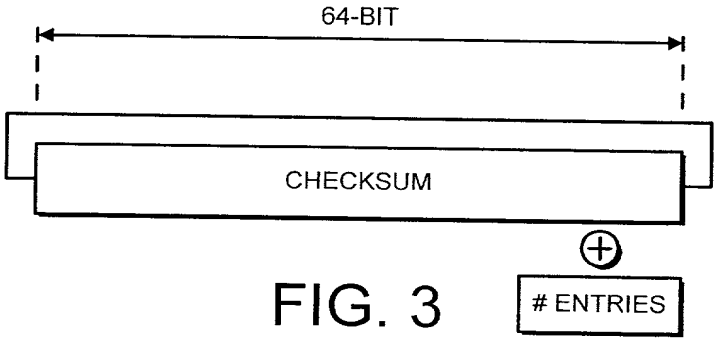

64-BIT
CHECKSUM
⊕
ENTRIES

FIG. 3

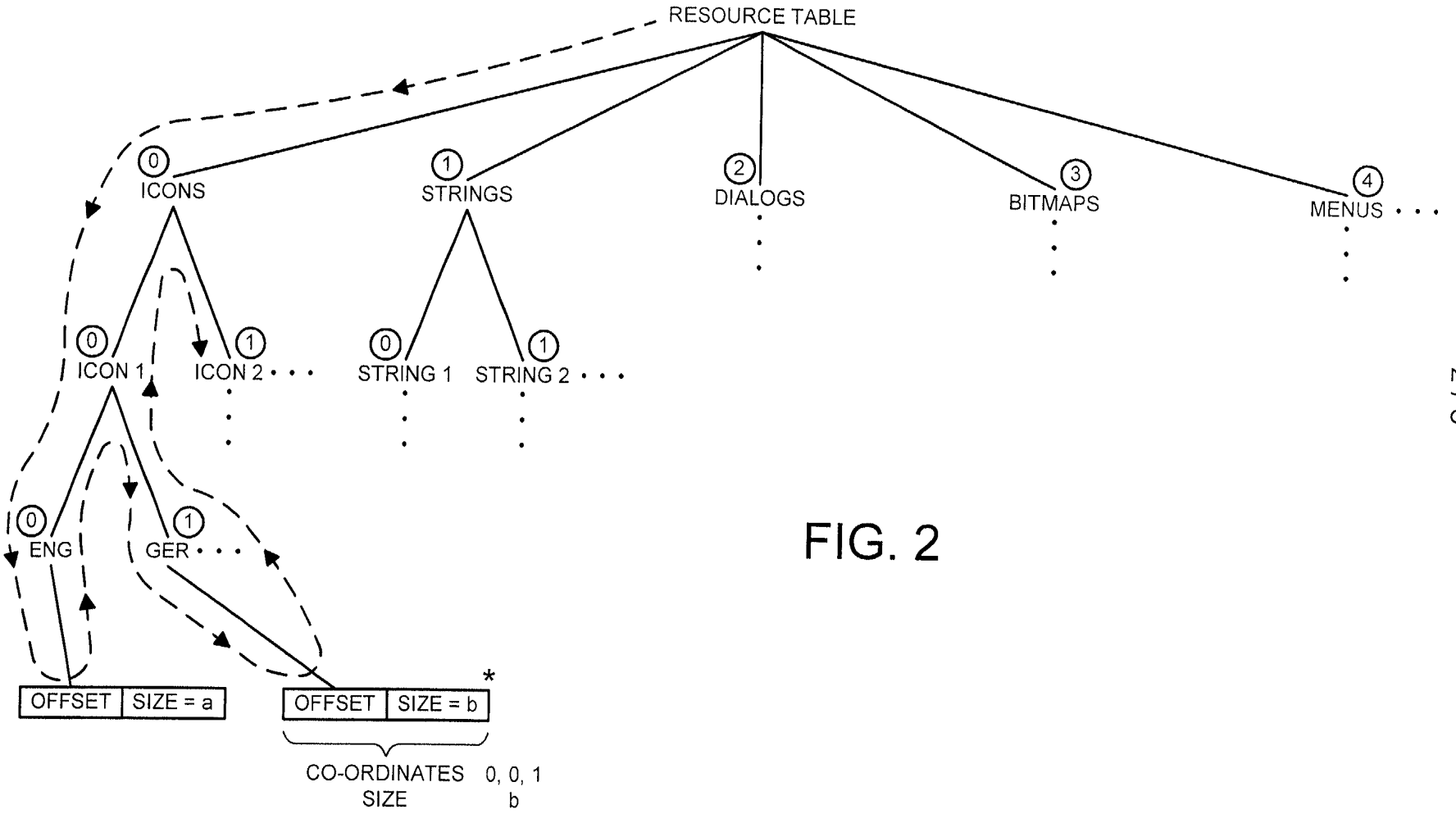
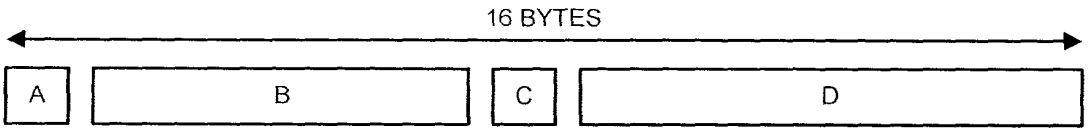

RESOURCE TABLE
0
ICONS
1
STRINGS
2
DIALOGS
3
BITMAPS
4
MENUS
0
ICON 1
1
ICON 2
0
STRING 1
1
STRING 2
0
ENG
1
GER
OFFSET
SIZE = a
OFFSET
SIZE = b
*
CO-ORDINATES
SIZE
0, 0, 1
b

FIG. 2

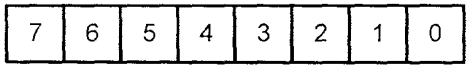
FINGERPRINT



A = 1 BYTE = CONTROL BYTE (SEE FIG. 4b)
B = 6 BYTES = ELIMINATION DATA (SEE FIG. 4c)
C = 1 BYTE = # ENTRIES PROCESSED
D = 8 BYTES = CHECKSUM

FIG. 4a

CONTROL BYTE



BITS 0 - 3 = RESERVED = 0
BITS 4 - 6 = 000 = RESERVED
001 = ELIMINATION DATA IS CO-ORD / SIZE
010 = ELIMINATION IS TIME STAMP
011 = ELIMINATION IS FILE LENGTH
100
101
110
111
} RESERVED
BIT 7 = RESERVED = 0

FIG. 4b

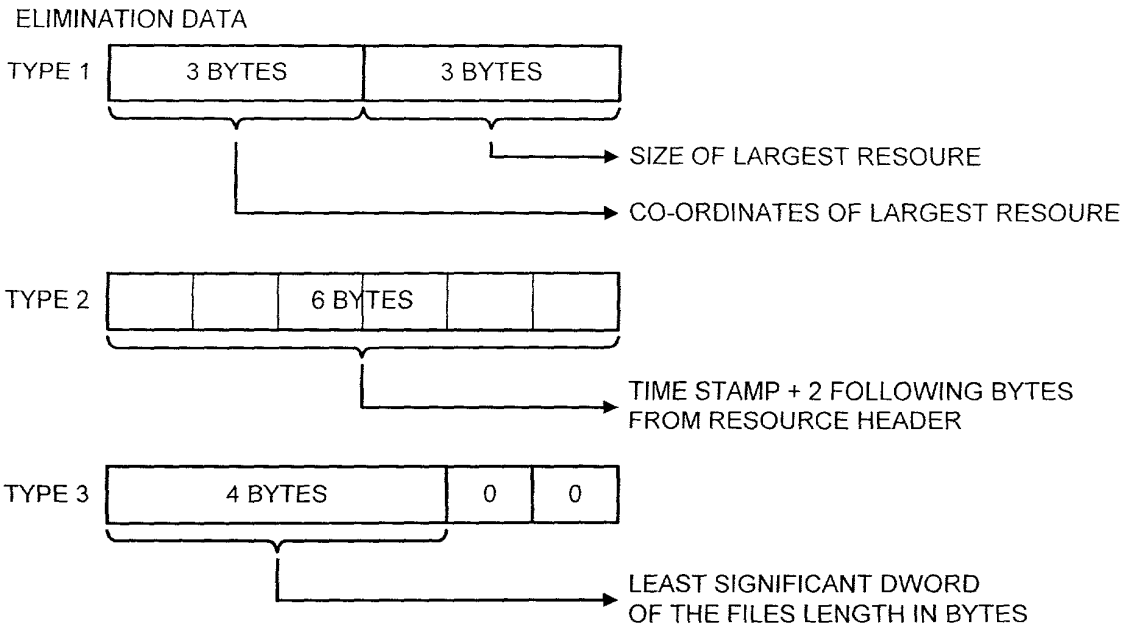

ELIMINATION DATA
TYPE 1
3 BYTES
3 BYTES
SIZE OF LARGEST RESOURE
CO-ORDINATES OF LARGEST RESOURE
TYPE 2
6 BYTES
TIME STAMP + 2 FOLLOWING BYTES
FROM RESOURCE HEADER
TYPE 3
4 BYTES
0
0
LEAST SIGNIFICANT DWORD
OF THE FILES LENGTH IN BYTES

FIG. 4c

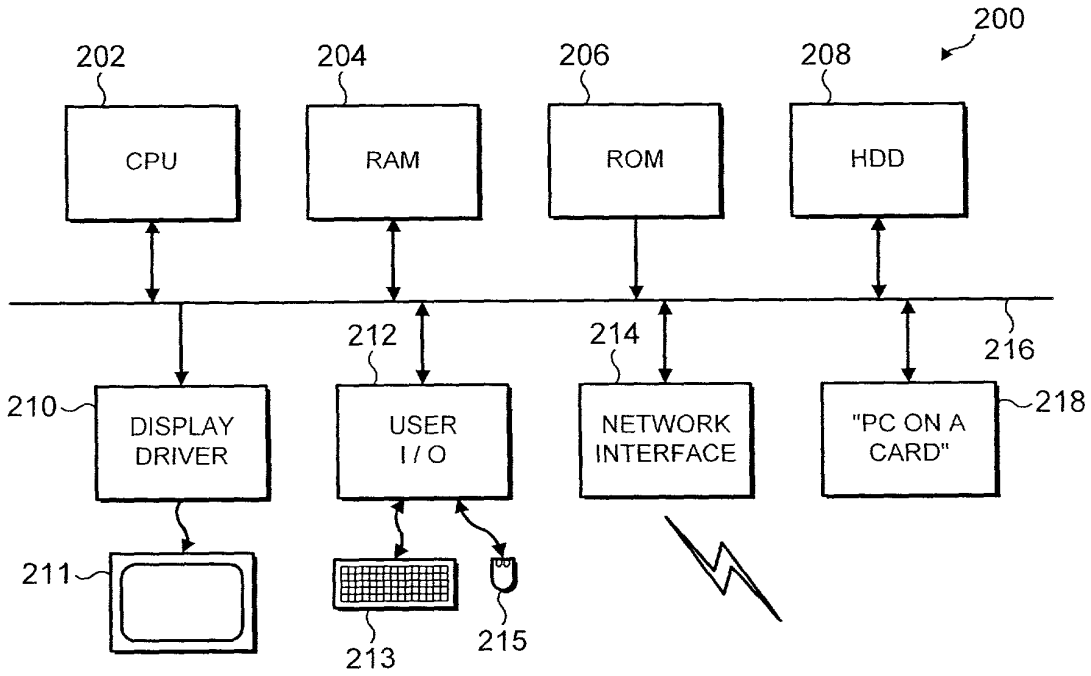

200
202
204
206
208
CPU
RAM
ROM
HDD
212
214
216
210
DISPLAY DRIVER
USER I / O
NETWORK INTERFACE
"PC ON A CARD"
218
211
213
215

FIG. 7

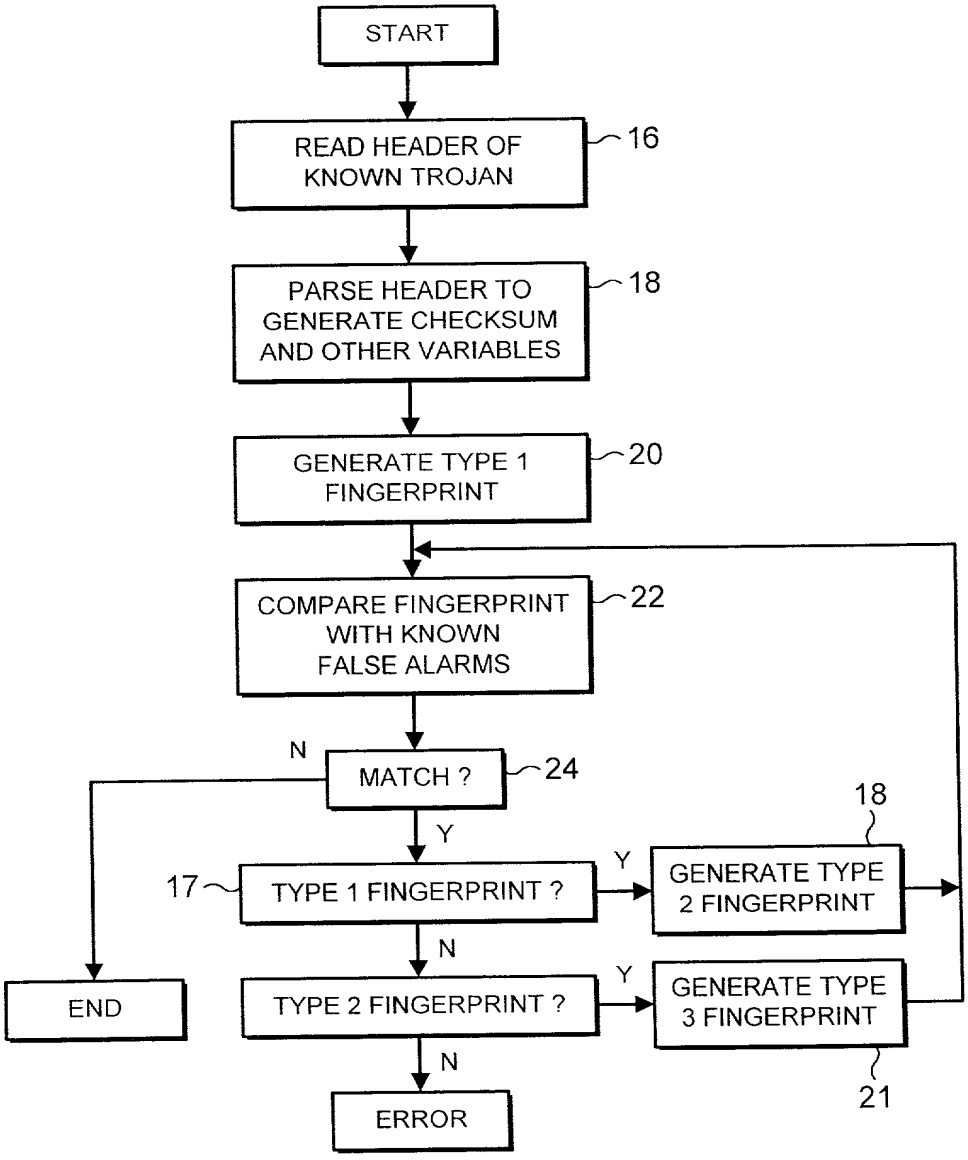

START
READ HEADER OF KNOWN TROJAN
16
PARSE HEADER TO GENERATE CHECKSUM AND OTHER VARIABLES
18
GENERATE TYPE 1 FINGERPRINT
20
COMPARE FINGERPRINT WITH KNOWN FALSE ALARMS
22
MATCH ?
24
N
Y
TYPE 1 FINGERPRINT ?
17
Y
GENERATE TYPE 2 FINGERPRINT
18
N
TYPE 2 FINGERPRINT ?
Y
GENERATE TYPE 3 FINGERPRINT
21
N
END
ERROR

FIG. 5

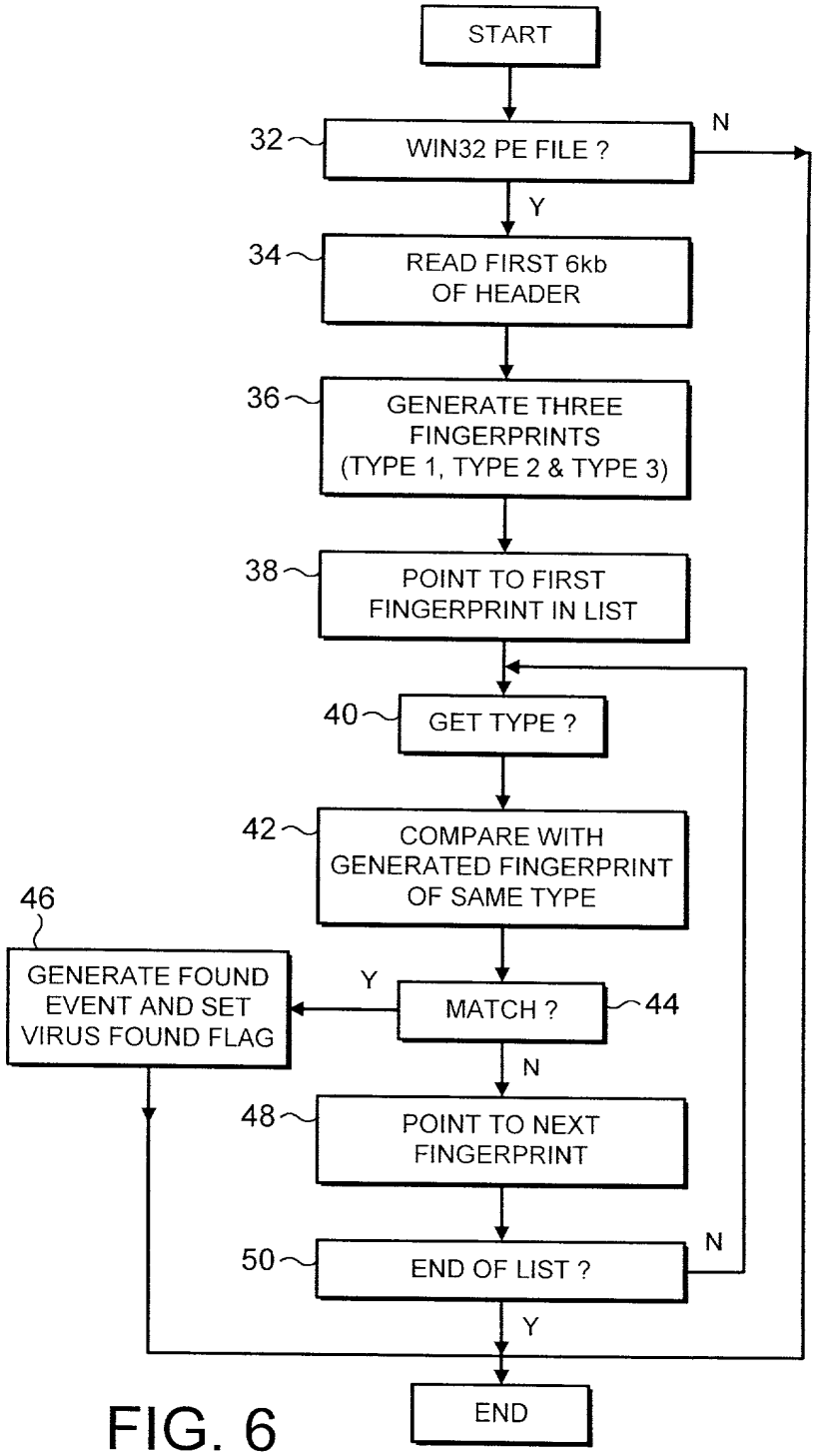

START
32
WIN32 PE FILE ?
N
Y
34
READ FIRST 6kb OF HEADER
36
GENERATE THREE FINGERPRINTS (TYPE 1, TYPE 2 & TYPE 3)
38
POINT TO FIRST FINGERPRINT IN LIST
40
GET TYPE ?
42
COMPARE WITH GENERATED FINGERPRINT OF SAME TYPE
46
GENERATE FOUND EVENT AND SET VIRUS FOUND FLAG
Y
MATCH ?
44
N
48
POINT TO NEXT FINGERPRINT
50
END OF LIST ?
N
Y
END

FIG. 6